011872005 **Image available**
WPI Acc No: 1998-288915/199826
XRPX Acc No: N98-227220

**Authentication information embedding system into image produced by digital camera - has region combining unit that combines first image region in image with second image region in which authentication information is embedded**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC ); IBM JAPAN LTD (IBMC ); MORIMOTO N (MORI-I); NUMAO M (NUMA-I); SHIMIZU S (SHIM-I)
Inventor: MORIMOTO N; NUMAO M; SHIMIZU S
Number of Countries: 030 Number of Patents: 009
Patent Family:

| Patent No | Kind | Date | Applicat No | Kind | Date | Week | |
|---|---|---|---|---|---|---|---|
| EP 845758 | A2 | 19980603 | EP 97309192 | A | 19971114 | 199826 | B |
| JP 10164549 | A | 19980619 | JP 96317526 | A | 19961128 | 199835 | |
| CA 2222346 | A | 19980528 | CA 2222346 | A | 19971127 | 199838 | |
| TW 342477 | A | 19981011 | TW 97110163 | A | 19970717 | 199908 | |
| KR 98041902 | A | 19980817 | KR 9749415 | A | 19970927 | 199937 | |
| US 6005936 | A | 19991221 | US 97918163 | A | 19970825 | 200006 | |
| SG 78279 | A1 | 20010220 | SG 973922 | A | 19971031 | 200117 | |
| JP 3154325 | B2 | 20010409 | JP 96317526 | A | 19961128 | 200122 | |
| KR 264635 | B1 | 20000901 | KR 9749415 | A | 19970927 | 200134 | |

Priority Applications (No Type Date): JP 96317526 A 19961128
Cited Patents: No-SR.Pub
Patent Details:

| Patent No | Kind | Lan | Pg | Main IPC | Filing Notes |
|---|---|---|---|---|---|
| EP 845758 | A2 | E | 13 | G06T-011/00 | |
| Designated States (Regional): AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI | | | | | |
| JP 10164549 | A | | 10 | H04N-007/167 | |
| CA 2222346 | A | | | H04N-001/387 | |
| TW 342477 | A | | | G06F-017/22 | |
| KR 98041902 | A | | | G06T-005/00 | |
| US 6005936 | A | | | H04L-009/00 | |
| SG 78279 | A1 | | | G06T-011/00 | |
| JP 3154325 | B2 | | 10 | H04N-007/167 | Previous Publ. patent JP 10164549 |
| KR 264635 | B1 | | | H04N-007/167 | |

Abstract (Basic): EP 845758 A

The system includes a region dividing unit (24) for dividing the image into a first image region and a second image region. An authentication information generating unit (29) generates authentication information from data in the first image region. A hiding unit (25) embeds the authentication information into the second image region by operating data in the second image region. A region combining unit (26) combines the first image region in the image with the second image region in which the authentication information is embedded.

ADVANTAGE - Enable image data to be verified without requiring storage of authentication information by verifier.

Dwg.2/5

Title Terms: AUTHENTICITY; INFORMATION; EMBED; SYSTEM; IMAGE; PRODUCE; DIGITAL; CAMERA; REGION; COMBINATION; UNIT; COMBINATION; FIRST; IMAGE; REGION; IMAGE; SECOND; IMAGE; REGION; AUTHENTICITY; INFORMATION; EMBED
Derwent Class: T01
International Patent Class (Main): G06F-017/22; G06T-005/00; G06T-011/00; H04L-009/00; H04N-001/387; H04N-007/167
International Patent Class (Additional): G06T-001/00; H04L-009/32; H04N-005/225; H04N-005/335; H04N-007/18
File Segment: EPI
Manual Codes (EPI/S-X): T01-J10A; T01-J10B; T01-J10D

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－164549

(43)公開日　平成10年(1998)６月19日

| (51)Int.Cl.* | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| H04N | 7/167 | | H04N | 7/167 | Z |
| | 5/225 | | | 5/225 | Z |
| | 7/18 | | | 7/18 | V |

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平8－317528

(22)出願日　平成８年(1996)11月28日

(71)出願人　592073101
日本アイ・ビー・エム株式会社
東京都港区六本木３丁目２番12号

(72)発明者　清水　周一
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

(72)発明者　招尾　雅之
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

(72)発明者　森本　典繁
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社東京基礎研究所内

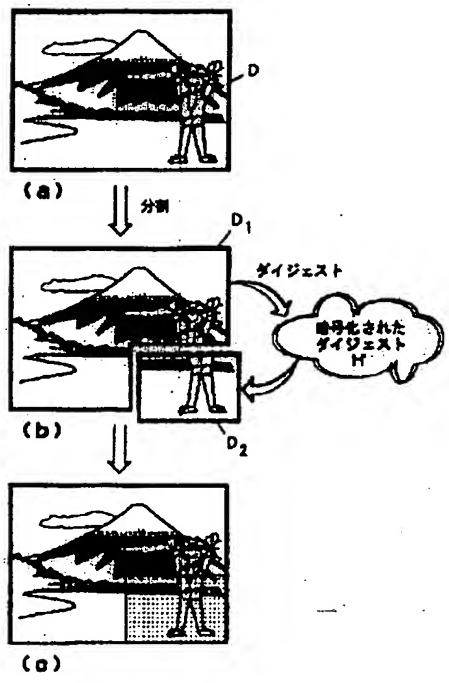
(74)代理人　弁理士　合田　潔　（外２名）

(54)【発明の名称】　認証情報を画像に隠し込むシステム及び画像認証システム

(57)【要約】　（修正有）

【課題】従来の画像へのデータハイディングでは検証するまで認証情報を添付しておく必要があり、それが欠落していると検証ができなかった。

【解決手段】画像を２つに分割し、一方の画像に隠し込む認証情報を他方の画像そのものから得るようにする。デジタル・カメラにおいて撮影された対象の画像データは、ハッシュ値を生成するための領域Ｄ１と生成されたハッシュ値Ｈを隠し込む領域Ｄ２とに分割される。ダイジェスト計算部はＤ１のデータからＨを計算し、デジタル・カメラごとに異なる秘密鍵で暗号化するなどして、Ｄ２に隠し込む。隠し込みは視覚的に認識できない程度に実空間や周波数空間で画素値を操作することにより行うことができる。Ｄ２には、Ｄ１からのデータの隠し込みの前に、タイム・スタンプやＧＰＳの位置情報といった付加情報を隠し込んでおくこともできる。



【特許請求の範囲】
【請求項１】第１の画像領域と，第２の画像領域とに画像を分割する領域分割手段と，前記第１の画像領域中のデータから認証情報を生成する認証情報生成手段と，前記第２の画像領域中のデータを操作することにより，前記認証情報を前記第２の画像領域中に隠し込むハイディング手段と，前記画像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成する領域合成手段とを有することを特徴とする認証情報を画像中に隠し込むシステム。
【請求項２】前記認証情報は，前記第１の画像領域中のデータのダイジェストであることを特徴とする請求項１に記載のシステム。
【請求項３】前記ダイジェストは，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項２に記載のシステム。
【請求項４】前記認証情報を暗号化する暗号変換手段をさらに有し，前記ハイディング手段は当該暗号化された認証情報を前記第２の画像領域中に隠し込むことを特徴とする請求項１に記載のシステム。
【請求項５】第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定する領域特定手段と，前記第１の画像領域中のデータから第１の認証情報を生成する認証情報生成手段と，前記第２の画像領域から，第２の認証情報を抽出する抽出手段と，前記第１の認証情報が前記第２の認証情報と一致する場合に，前記画像が改変されていないと判断する認証手段とを有することを特徴とする画像認証システム。
【請求項６】前記認証手段は，前記第１の認証情報が前記第２の認証情報と一致しない場合には，前記画像が改変されていると判断することを特徴とする請求項６に記載のシステム。
【請求項７】前記第１の認証情報は，前記第１の画像領域中のデータのダイジェストであることを特徴とする請求項５に記載のシステム。
【請求項８】前記ダイジェストは，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項６に記載のシステム。
【請求項９】前記第２の認証情報は暗号化されており，前記第２の認証情報を復号化する復号変換手段をさらに有し，かつ，前記認証手段は，当該復号化された認証情報が前記第１の認証情報と一致する場合に，前記画像が改変されていないと判断することを特徴とする請求項５に記載のシステム。
【請求項１０】第１の画像領域と，第２の画像領域とに画像を分割するステップと，前記第１の画像領域中のデータから認証情報を生成するステップと，前記第２の画像領域中のデータを操作することにより，前記認証情報を前記第２の画像領域中に隠し込むステップと，前記画像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成するステップとを有することを特徴とする認証情報を画像中に隠し込む方法。
【請求項１１】第１の画像領域と，データを操作することにより情報が隠し込まれた第２の画像領域とを画像中において特定するステップと，前記第１の画像領域中のデータから第１の認証情報を生成するステップと，前記第２の画像領域から，第２の認証情報を抽出するステップと，前記第１の認証情報が前記第２の認証情報と一致する場合に，前記画像が改変されていないと判断するステップとを有することを特徴とする画像の同一性を認証方法。
【請求項１２】光学系と，前記光学系を介して入力された光を電気信号に変換することにより，画像のアナログ信号を出力する変換器と，前記アナログ信号に応じて，画像のデジタル信号を生成する信号処理手段と，前記デジタル信号に応じて，画像を，第１の画像領域と，第２の画像領域とに分割する領域分割手段と，前記第１の画像領域中のデータから認証情報を生成する認証情報生成手段と，前記認証情報を暗号化する暗号変換手段と，前記第２の画像領域中のデータを操作することにより，暗号化された認証情報を前記第２の画像領域中に隠し込むハイディング手段と，前記画像における前記第１の画像領域と前記認証情報が隠し込まれた前記第２の画像領域とを合成する領域合成手段とを有することを特徴とするデジタル・カメラ。
【請求項１３】前記認証情報は，前記第１の画像領域中のデータのハッシュ値であることを特徴とする請求項１２に記載のデジタル・カメラ。
【発明の詳細な説明】
【０００１】
【発明の属する利用分野】本発明は，画像のダイジェストを隠し込むシステムに係り，特に，撮影された画像の認証情報をこの画像に付加するデジタル・カメラに関する。
【０００２】
【従来の技術】最近，デジタル・カメラが急速に普及しつつある。デジタル・カメラは，景色などを撮影し，これをデジタル・データとしてメモリー・カードなどに保存するものである。デジタル・カメラの急速な普及の理由は，本体価格の低下やその優れた携帯性にあることは当然であるが，より重要なことは，撮影された写真をデジタル画像として保存できる点にある。デジタル・データは，コンピュータにより，ユーザの好みに応じて内容を容易に加工することでき，かつネットワークなどを介して容易に流通させることができる。従って，このようなデジタル画像を簡単に得ることができるデジタル・カメラの必要性は，今後ますます大きくなるものと期待されている。

【0003】その一方で，デジタル・データは，痕跡が残らないように合成などの改ざんを行うことが容易であるため，撮影されたデジタル画像の証拠としての信頼性が問題となる場合がある。このような問題は，一般ユーザによる趣味的な撮影程度であればあまり生じないであろうが，ビジネスにおける撮影では大きな問題となり得る。例えば，建設工事の工事記録としてデジタル・カメラを用いたり，発注元と請負先との間で，ネットワークを通じて，撮影されたデジタル画像を送受信する場合である。これらの場合，撮影されたデジタル画像は，その内容の同一性を認証できて，初めて証拠写真としての機能を発揮することができる。従って，撮影されたデジタル画像の同一性に関する認証情報を付加できるデジタル・カメラへの期待は大きい。

【0004】図1は，従来のデジタル・カメラの画像処理系のブロック図である。撮影された対象は，光学系11を介して，CCD12により電気的なアナログ信号に変換される。この信号は信号処理部13により処理され，デジタル信号である画像データDとして出力される。この生成された画像データDは，ダイジェスト計算部14に入力される。ダイジェスト計算部14は，画像全体のデータのハッシュ値Hを計算する。ハッシュ値は，画像データに基づいた演算により画像の特徴を示す一意に定まる値（ダイジェスト）である。ダイジェストとしてのハッシュ値Hは，画像内容が異なれば，相違する値となる。暗号変換部15は，ハッシュ値Hを秘密鍵SKを用いて暗号化し，暗号化されたハッシュ値H'を出力する。この暗号化されたハッシュ値H'が認証情報であり，これは画像データDとは別ファイルの形で添付される。

【0005】画像データがオリジナルの画像データと同一であるか，換言すると，画像データが改ざんされていないかを判断するためには，以下の情報が必要である。
（1）画像データ
（2）認証情報（別ファイルとして画像データに添付）
（3）秘密鍵SKに対応した公開鍵PK（権限を有する者から別途入手）

【0006】改ざんを検出する者は，まず認証しようとする画像データのハッシュ値$H_1$を計算する。次に添付ファイル中の認証情報からハッシュ値$H_2$を特定する。この認証情報は，原画像Dのハッシュ値Hを秘密鍵SKにより暗号化したもの（ハッシュ値H'）なので，そのままではハッシュ値$H_2$を特定することはできない。そこで，秘密鍵SKに対応した公開鍵PKを保管している権限ある者から，この公開鍵PKを入手し，これに基づいて，認証情報を復号化する。そして，得られたハッシュ値$H_2$を，計算したハッシュ値$H_1$と比較する。認証対象としての画像が原画像Dと同一であれば，両者の値は一致するはずである。ダイジェストとしてのハッシュ値は，画像の内容が異なれば，その値が異なっているはずだからである。従って，ハッシュ値が一致する場合には，同一性を認証し，異なる場合には，改ざんされたものと判断する。

【0007】
【発明が解決しようとする課題】このように，従来の技術における同一性の認証は，画像データとは別に認証情報を添付し，検証時に認証情報が添付されていることを前提に認証を行うものである。従って，認証情報が欠落している場合にはもはや検証を行うことができない。従って，検証者は，認証情報の保管・管理に細心の注意を払わねばならなかった。

【0008】そこで，本発明の目的は，認証情報を画像データと一体不可分な形式で供給することが可能な新規な方式を提案することである。

【0009】また，本発明の別の目的は，検証者が認証情報を保管することなく，画像データの検証を可能にすることである。

【0010】さらに，本発明の別の目的は，画像データの画質を劣化させることなく，画像中に認証情報を隠し込むことである。

【0011】
【課題を解決するための手段】上記課題を解決するために，第1の発明は，画像を第1の画像領域及び第2の画像領域に分割する領域分割手段と，第1の画像領域のデータから認証情報を生成する認証情報生成手段と，第2の画像領域中のデータを操作することにより，認証情報を第2の画像領域中に隠し込むハイディング手段と，画像における第1の画像領域と認証情報が隠し込まれた第2の画像領域とを合成する領域合成手段とを有する認証情報を画像の一手段に隠し込むシステムを提供する。

【0012】第2の発明は，第1の画像領域と，データを操作することにより情報が隠し込まれた第2の画像領域とを画像中において特定する領域特定手段と，第1の画像領域中のデータから第1の認証情報を生成する認証情報生成手段と，第2の画像領域から，第2の認証情報を抽出する抽出手段と，第1の認証情報が第2の認証情報と一致する場合に，画像が改変されていないと判断し，一致しない場合には，画像が改変されていると判断する認証手段とを有する画像認証システムを提供する。

【0013】第3の発明は，第1の画像領域と，第2の画像領域とに画像を分割するステップと，第1の画像領域中のデータから認証情報を生成するステップと，第2の画像領域中のデータを操作することにより，認証情報を第2の画像領域中に隠し込むステップと，画像における第1の画像領域と認証情報が隠し込まれた第2の画像領域とを合成するステップとを有する認証情報を画像の一手段に隠し込む方法を提供する。

【0014】第4の発明は，第1の画像領域と，データを操作することにより情報が隠し込まれた第2の画像領域とを画像中において特定するステップと，第1の画像

領域中のデータから第1の認証情報を生成するステップと，第2の画像領域から，第2の認証情報を抽出するステップと，第1の認証情報が第2の認証情報と一致する場合に，画像が改変されていないと判断するステップとを有する画像の同一性を認証方法を提供する。

【0015】

【作用】このような構成では，（第2の）認証情報が第2の画像領域中に隠し込まれる。（第2の）認証情報は，画像の同一性を認証するための情報であり，第1の画像領域の内容によって異なる固有なものである。もし，第1の画像領域内のデータが改変された場合，改変されたデータに基づき生成される第1の認証情報は，第2の画像領域中に隠し込まている第2の認証情報とは異なる値となる。従って，第2の画像領域中に隠し込まれた第2の認証情報を抽出し，それを第1の画像領域から新たに生成した第1の認証情報と比較すれば，画像が改変されているか否かを検証することができる。

【0016】

【発明の実施の形態】

［デジタル・カメラ］図2は，本実施例におけるデジタル・カメラの画像処理系のブロック図である。撮影された対象は，光学系21を介して，CCD22により電気的なアナログ信号に変換される。この信号は，信号処理部23，領域分割部24，ハイディング部25及び領域合成部26を有する画像処理部27により処理され，デジタル信号である画像データD'として出力され，メモリー・カード等の記憶部28に保存される。この画像データD'は，ハイディング部25により，画像データD中の所定の画像領域にハッシュ値が隠し込まれているため，画像データDと完全に同一なデータではないが，視覚的にその相違を見分けることはできない。

【0017】信号処理部23の出力である画像データDは，領域分割部24により，2つの領域に切り分けられる。図3は，画像領域の分割及び合成を説明するための概念図である。同図（a）のような画像Dは，ハッシュ値生成のための入力値を与える画像領域$D_1$と生成されたハッシュ値Hを埋め込む画像領域$D_2$とに分割される（同図（b）参照）。本実施例において，画像領域$D_2$は画像の右下の40×40画素で構成され，理想的には160ビットの情報を隠し込むことが可能である。

【0018】領域分割部23により分割された画像領域$D_1$は，認証情報生成部としてのダイジェスト計算部29に入力される。ダイジェスト計算部29は，切り取られた画像領域$D_1$全体のデータのハッシュ値Hを認証情報として計算する。ハッシュ値は，画像データに基づいた演算により画像の特徴を示すダイジェストである。ダイジェストとは，画像データの特徴を示す要約であり，ダイジェストとしてのハッシュ値Hは，画像内容の一画素の変更に対しても敏感に反応し，全く異なる値に変わるという性質を有する。従って，特に自然画像データとほぼ1対1の関係にある数値であると考えることができる。

【0019】ハッシュ値Hは，具体的には以下の式で表現される。

【数1】

$$H=H1(d[0]//d[1]//d[2]//\cdots//d[i])$$

【0020】ここで、H1はハッシュ関数である。また、演算子「//」は、メッセージ配列の各要素をつなげるという意味である。また，d[i]は，画像領域$D_1$中に含まれる各画素値を示している。この具体的な演算は、例えば、配列要素が有するデータの排他的論理和でもよい。但し、排他的論理和とした場合には、メッセージ配列値の順序は計算結果に反映されない。例えば、CRC(Cyclic Redundancy Check)という方法を用いれば、この順序関係を反映することができる。このアルゴリズムは、、チェックサムを計算するためのアルゴリズムの一つで、データ列の内容及びデータ列の順序に依存した出力を生成する。

【0021】このハッシュ関数H1は、バイト長が$B_a$バイトである入力（配列値d[i]）に対して、それと異なるバイト長Kの出力（ハッシュ値）を求める関数である。この関数は一方向関数であるから、H(x)=yにおいて、yからxを推定することは、事実上不可能である。ハッシュ値は、データ・ハイディングの際に単に初期値として用いられるものであり、異なる入力に対して異なる出力が事実上保証されていれさえすればよい。従って、ハッシュ値の値自身には特別な意味はない。重要なことは、その演算により配列の特徴を示す値を出力すること、つまり配列要素全体の内容に基づいてハッシュ値が一意に定まり、かつその値が配列全体の内容により異なることである。

【0022】暗号変換部30は，ハッシュ値Hを秘密鍵SKを用いて暗号化し，暗号化されたハッシュ値H'を出力する。この暗号化されたハッシュ値H'が認証情報である。秘密鍵SKは，デジタル・カメラごとに異なる鍵を用いるものとし，カメラ内部に保持されている

【0023】認証情報として暗号化されたハッシュ値H'は，画像処理部27中のハイディング部25に送られる。ハイディング部25は，画像領域中$D_2$のデータを操作することにより，ハッシュ値H'を画像領域$D_2$中に隠し込む。隠し込みは，実空間又は周波数空間において，画像領域$D_2$中のデータ（例えば画素値）を操作することにより行うことが可能である。埋め込みは様々な方法が考えられるが，その具体例については後述する。なお，これに関しては，特願平8－159330号（当方整理番号JA996－044）及び特願平8－272721号（当方整理番号JA996－074）にも詳細に説明されている。

【0024】画像領域$D_2$中には，ハッシュ値H'を隠し込むため，その領域内のデータを操作しているので，

その部分における画質は，原画像と多少相違している。しかしながら，視覚的にはこのような相違を認識することはほとんど不可能なので，画質の視覚的な劣化は生じない。

【００２５】領域合成部２６は，原画像中の画像領域$D_1$とハッシュ値H'が隠し込まれた画像領域$D_2$とを合成する（図３（ｃ）参照）。そして，この合成された画像データD'を記憶部２８中に保存する。

【００２６】上記の説明から明らかなように，画像領域の分割は，ダイジェストの計算とは関係しない埋め込む領域を特定するために行われる。もし，画像領域を分割せずに，画像全体のダイジェストを計算して，その結果を隠し込んだとすると，この隠し込み後の画像全体の新たなダイジェストは，埋め込まれている元のダイジェストと一致しなくなる。従って，このような方法では，画像の同一性の認証を行うことができない。そこで，ダイジェストを隠し込む画像領域は，ダイジェスト計算の対象としないことにより，計算されたダイジェストと隠し込まれているダイジェストとの一致を保証しているのである。このような観点において，画像領域$D_2$の部分だけを黒や白等の単色で塗りつぶした原画像Dを画像領域$D_1$としてもよい。この場合，一部が塗りつぶされた原画像Dのダイジェストを計算して，それを画像領域$D_2$に隠し込む。これにより，隠し込み後においてもダイジェストの一致を保証することができる。

【００２７】なお，本実施例におけるデジタル・カメラは，撮影カメラのＩＤ，撮影の日付等のタイム・スタンプ，ＧＰＳで測定される位置情報といった付加情報を画像領域$D_1$中に隠し込んでおいてもよい。この場合には，まず，画像領域$D_1$中に付加情報を隠し込んんで，その後に，その結果のハッシュ値H'を画像領域$D_2$に隠し込むことが重要である。なぜなら，付加情報を埋め込む前の画像のハッシュ値H'を画像領域$D_2$に隠し込むと，その後の付加情報の隠し込みにより，ハッシュ値が相違してしまうため，同一性の認証ができなくなるからである。

【００２８】なお，画像領域$D_2$は，上記の実施例のように一箇所に集中している必要はなく，位置系列生成アルゴリズムを用いて分散して存在させてもよいし，Low Bitの一部だけ用いてもよい。

【００２９】［画像認証システム］次に，隠し込まれた認証情報を用いて，デジタル・カメラで撮影された画像の同一性認証を行うシステムについて説明する。同一性を検証しようとする者は，以下の情報を有している必要がある。認証情報は，画像中に一体不可分な状態で隠し込まれているため，別ファイルの形式で保管している必要はない点に留意されたい。

（１）画像データM'

（２）秘密鍵ＳＫに対応した公開鍵ＰＫ（権限を有する者から別途入手）

【００３０】図４は，本実施例における画像の同一性認証システムのブロック図である。領域特定部４１は，ハッシュ値H'が隠し込まれている画像D'において，画像領域$D_1$と画像領域$D_2$とを特定する。画像領域$D_1$は，ハッシュ値を生成するためのデータを与える領域であり，画像領域$D_2$は，上述の認証情報としてのハッシュ値H'が隠し込まれている領域である。

【００３１】ダイジェスト計算部４２は，画像領域$D_1$中のデータに基づいて，ハッシュ値を新たに計算する。また，ダイジェスト抽出部４３は，画像領域$D_2$から，認証情報として隠し込まれている暗号化されたハッシュ値H'を抽出する。具体的な抽出方法は，具体的な埋め込む方法と共に後述する。

【００３２】復号変換部４４は，抽出されたハッシュ値H'を，公開鍵ＰＫを用いて復号する。この公開鍵ＰＫは，秘密鍵ＳＫに対応して一意に定まる入手可能な鍵であり，これを保管している権限ある者から入手する必要がある。

【００３３】認証部４５では，ダイジェスト計算部４２により新たに計算された画像領域$D_1$中のデータに基づいたハッシュ値と，復号変換部４４により得られたハッシュ値H'とを比較することにより同一性の認証を行う。すなわち，ハッシュ値が一致する場合は，画像が改ざんされていないと判断する。また，ハッシュ値が一致しない場合は，画像が改ざんされていると判断する。ハッシュ値が一致しないケースが生じるのは以下の２つの少なくとも一方に該当する場合である。

（１）画像領域$D_1$が改ざんされている場合
画像領域$D_1$から新たに再測したハッシュ値が変わるので，画像領域$D_2$中に隠し込まれたハッシュ値Hと一致しなくなる。

（２）画像領域$D_2$が改ざんされている場合
画像領域$D_2$に隠し込まれたハッシュ値Hが変わるので，画像領域$D_1$から再測したハッシュ値と一致しなくなる。

【００３４】本実施例によれば，データ・ハイディング技術を用いることにより，認証情報が画像中に一体化して隠し込まれているため，認証情報を画像データに別ファイルとして添付する必要がない。従って，検証者が認証情報を特に保持していなくとも検証を実施することができる。

【００３５】また，公開鍵暗号方式を用いて，認証情報を暗号化（スクランブル）しているので，悪意の第三者による認証情報の書き換えを事実上不可能にすることができる。さらに，ある公開鍵ＰＫは，ただ１つの秘密鍵ＳＫに対応している。従って，秘密鍵ＳＫは，デジタル・カメラごとに相違させることにより，そのデジタル画像がどのデジタル・カメラで撮影されたのかを認証することも可能である。

【００３６】なお，デジタル・カメラを開封して本体内

部の保持情報への不正なアクセスに対抗するために，携帯電話等で用いられている耐タンパー・モジュールなどのデバイスを利用することが有効である。このような不正アクセスが行われた場合，秘密鍵ＳＫが盗難されたものとみなして，その秘密鍵ＳＫによる画像データについては，ダイジェストが一致した場合でも，改ざんされたもの判定する。このようにすることで，第三者の不正な行為による被害を避けることができる。

【００３７】なお，上記実施例は，デジタル・カメラについて説明したが，本発明はこれに限定されるものではなく，デジタル・ビデオなどのデジタル・システムに広く利用できることは当然である。

【００３８】

【実施例】ここでは、隠ぺいの対象となるデータをあるあるメディア・データ中に埋め込む方法及び逆に埋め込まれたデータを抽出する方法の一例であるピクセル・ブロック・コーディング(Pixel Block Coding)（以下、ＰＢＣという）について説明する。ＰＢＣを用いた場合、データをハイディング及び抽出は、以下の述べるようなある変換規則に従って処理される。

【００３９】［基本アルゴリズム］一般的に、隣接した２つの画素の画素値等の１次特性は互いに高い相関関係を有している。従って、画素値を入れ変えたとしても、画像が視覚的に認識できる程度の劣化は生じない。この性質に鑑みて、本アルゴリズムは、少なくとも１つの画素を有する画像領域をピクセル・ブロックとして定義し、ある変換規則に基づき意図的に隣接したピクセル・ブロックの特性値を入れ替えることで、１ビットのデータを隠ぺいする。すなわち、データは、隣接するピクセル・ブロックの特性値の入れ替えにより表現される。また、データの抽出時には、この変換規則に基づき決定される抽出規則に従って、データを抽出する。

【００４０】ビット情報は、隣接した２つのピクセル・ブロックの特性値（例えば、輝度値）を以下の変換規則に従って入れ替えること表現される。

【００４１】ビット・オン <;1>;:　一方のピクセル・ブロック（$PB_1$）の特性値が他方（$PB_2$）の特性値より大きい場合

ビット・オフ <;0>;:　一方のピクセル・ブロック（$PB_1$）の特性値が他方（$PB_2$）の特性値より小さい場合

【００４２】また、ビット情報は、以下の抽出規則に従って、隣接した２つのピクセル・ブロックの特性値（例えば、輝度値）を比較することにより抽出される。

【００４３】一方のピクセル・ブロック（$PB_1$）の特性値が他方（$PB_2$）の特性値より大きい場合：ビット・オン <;1>;

一方のピクセル・ブロック（$PB_1$）の特性値が他方（$PB_2$）の特性値より小さい場合：ビット・オフ <;0>;

【００４４】図５は、ＰＢＣを用いたデータのハイディング及び抽出を説明するための図である。ピクセル・ブロック$PB_1$、$PB_2$は例えば３×３画素のように複数の画素の集合として定義してもよいし、１画素を１ピクセル・ブロックと定義することも可能である。隣接するピクセル・ブロックは高い相関を有しているので、それらの位置を入れ替えたとしても、画像が視覚的に認識できる程度に劣化したとは感じることはないであろう（図５（ａ））。

【００４５】オリジナル画像におけるピクセル・ブロックの位置が同図（ｂ）である場合を考える。まず、二つのピクセル・ブロックの特性値を比較し、その結果、$PB_1$の特性値の方が$PB_2$の特性値よりも大きいとする。オリジナルにデータ”１”を隠ぺいする場合、ピクセル・ブロックの特性値が、変換規則におけるデータ”１”の条件を既に満たしているので、これらのブロックの特性値の入れ替え行われない。データを抽出する際、$PB_1$の特性値が大きい場合はデータ”１”であると抽出規則が定めているので、データ”１”が抽出される。

【００４６】一方、オリジナルにデータ”０”を隠ぺいする場合、オリジナルにおけるピクセル・ブロックの特性値の関係が、変換規則におけるデータ”０”の条件を満たさないので、ピクセル・ブロックの特性値を入れ替える。しかしながら、この入れ替えは視覚的には認識できない。抽出時は、抽出規則に従って、これらのブロックの特性値の関係からデータ”０”が抽出される。

【００４７】このようにＰＢＣでは、隠ぺいの対象となる情報を隠ぺいするのに十分な数のピクセル・ブロックを画像中から選択する。そして選択された一のピクセル・ブロックとそれに隣接するピクセル・ブロックのペアを作ることにより、このペアの列を生成する。そして、列の先頭から順々に隠ぺい対象となるビットを隠ぺいしていく。

【００４８】この列は、第１の実施例における状態系列Ｓに対応付けてもよい。例えば、ピクセル・ブロックを第１の実施例におけるメディア配列Ｍの配列要素Ｍに対応付ける。ハイディング作業において逐次的に生成された状態系列の各配列要素（状態値$S_j$）及びそれに隣接するメディア配列値とでペアを作る。そして、このペアに対して上記処理を施すことが考えられるまた、ある乱数の種（シード）から発生される疑似乱数列をもとに決定することももちろん可能である。

【００４９】抽出時には、ハイディング時と同じブロック列をスキャンする。それぞれのペアがビット・オンを表すかオフを表すかを抽出規則に従って１ビットずつ集めることで全体のメッセージを抽出する。もし、ペアであるピクセル・ブロックの特性値が同じであるならば、そのペアはハイディング時と同様にスキップする。ブロック列あるいはその列生成方法を秘密にすれば、隠ぺいされた情報を他人から隠すことができる。

【００５０】なお，ＰＢＣにおいて，埋め込み位置は，画質及び抽出精度に鑑みて決定するのが好ましい。すな

わち，埋め込み対象となっているペアを構成するピクセル・ブロックの特性値の差があまり大きいと，入れ替え操作により画質が劣化するおそれがある。このような画質の劣化を抑制するために，第1の閾値（上限）を設けておき，特性値の差がその閾値以上であれば，そのペアにはビットを埋め込まないようにすることが好ましい。

【００５１】また，特性値の差が小さければ，入れ替え操作による画質の劣化はほとんど生じないが，逆にノイズの影響により大小関係が反転してしまい，抽出時に埋め込まれたビットが抽出できないおそれがある。従って，抽出精度の低下を抑制するためには，第2の閾値（下限）を設けておき，特性値の差がその閾値以下であれば，そのペアにはビットを埋め込まないようにすることが好ましい。

【００５２】これらのケースに該当するペアには何も操作を施すことなくスキップする。そして、隠べいすべきビット情報を先送りして、次のペアを対象に隠べいする。

【００５３】［ブロックの特性値］特性値として、ピクセル・ブロックの１次特性に関する値及び２次特性に関する値を用いることできる。１次特性は、ピクセル・ブロックの輝度や色度のように画素値の直接的なパラメータである。また、２次特性は、前記パラメータの平均値や分散といった統計的な性質を示す値のように、１次特性をを分解することで得られる。さらに，特性値は，複数の画素値からなる配列と所定の配列（マスク）との演算結果としてもよく，周波数変換を行うことにより得られる特定の要素値とすることも可能である。一般に、１次特性は隣接する２つのピクセル・ブロックにおいて高い相関関係を有している。これに対して、２次特性は隣接しない離れた二つのブロックにおいて高い相関関係を有し得る。従って、ｐＢＣの対象となるピクセル・ブロックは、必ずしも隣接するブロックに限定されない点に留意されたい。

【００５４】

【効果】このように本発明によれば，認証情報は画像データと一体不可分な形式，すなわち画像中に隠し込まれた形式で供給されるので，検証者は認証情報を別に保管しておく必要がない。このような認証情報の隠し込みを行っても画像データの画質を劣化させることはない。

【図面の簡単な説明】

【図１】従来のデジタル・カメラの画像処理系のブロック図である。

【図２】本実施例におけるデジタル・カメラの画像処理系のブロック図である。

【図３】本実施例における画像の同一性認証システムのブロック図である。

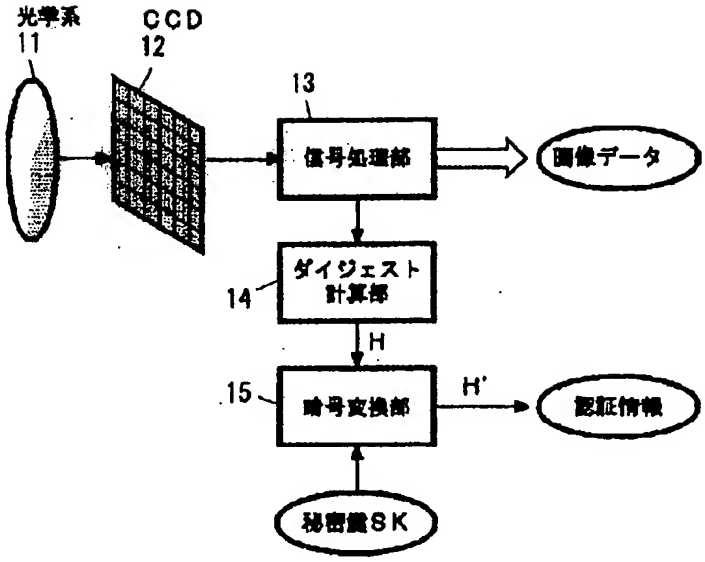
【図４】本実施例における画像の同一性認証システムのブロック図である。

【図５】ＰＢＣを用いたデータのハイディング及び抽出を説明するための図である。

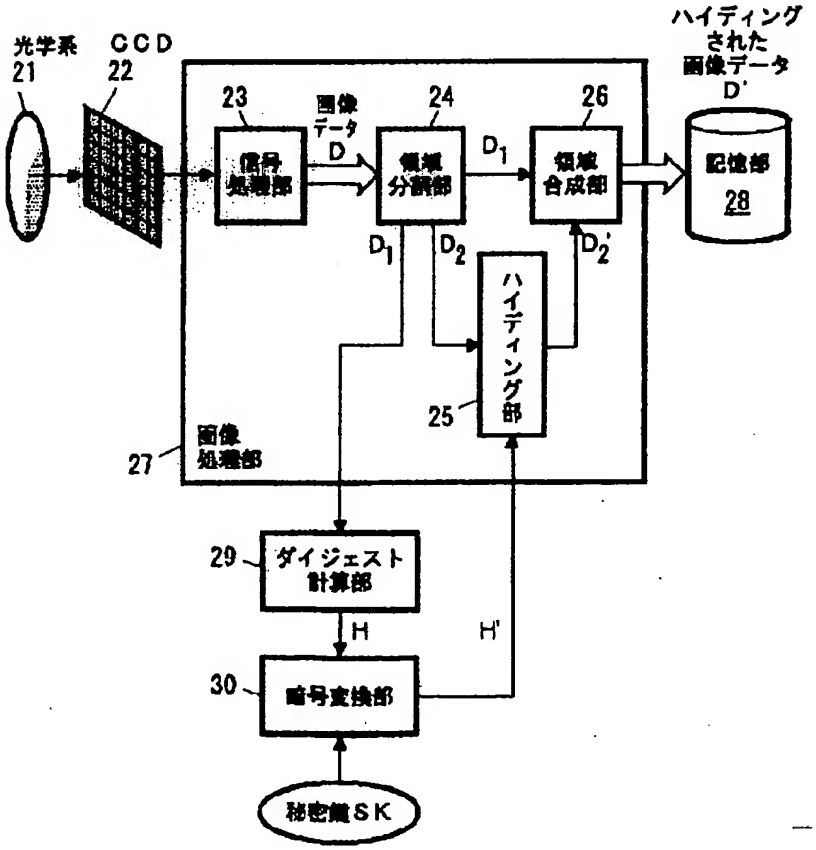
【符号の説明】

２１・・・光学系
２２・・・ＣＣＤ
２３・・・信号処理部
２４・・・領域分割部
２５・・・ハイディング部
２６・・・領域合成部
２７・・・画像処理部
２８・・・記憶部
２９・・・ダイジェスト計算部
３０・・・暗号変換部

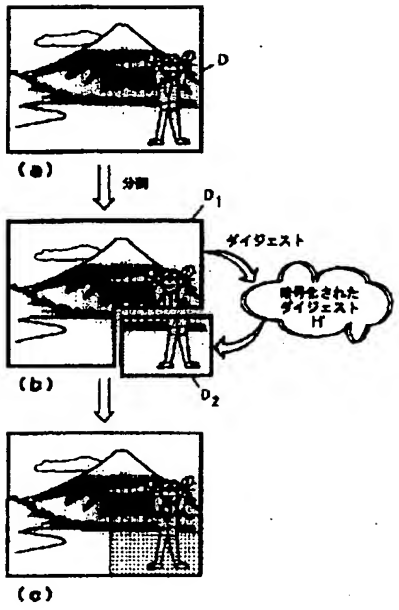
【図1】


光学系
11
CCD
12
13
信号処理部
画像データ
ダイジェスト
計算部
14
H
15
暗号変換部
H'
認証情報
秘密鍵SK

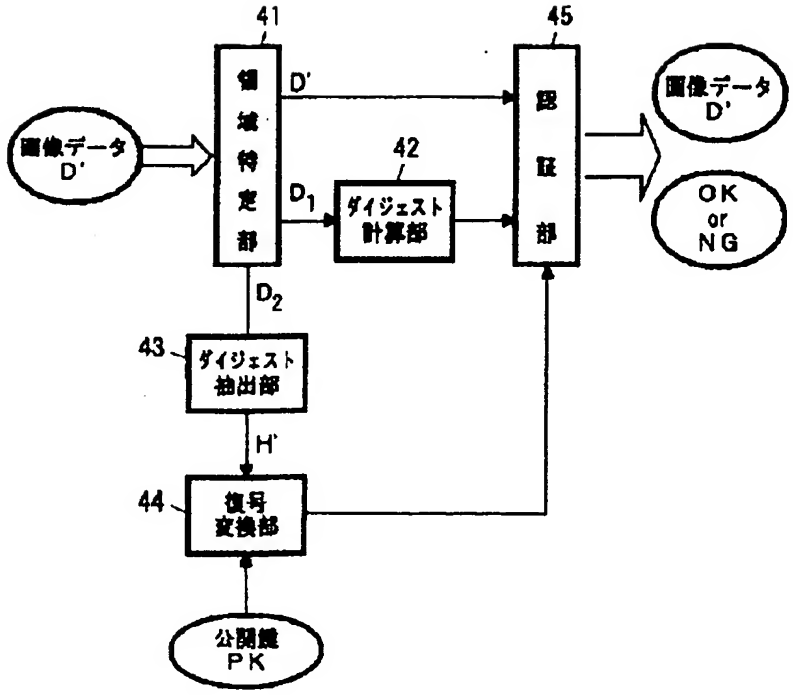
【図2】


光学系
21
CCD
22
23
信号
処理部
画像
データ
D
24
領域
分割部
D1
26
領域
合成部
ハイディング
された
画像データ
D'
記憶部
28
D1
D2
D2'
ハイディング
部
25
画像
処理部
27
29
ダイジェスト
計算部
H
H'
30
暗号変換部
秘密鍵SK

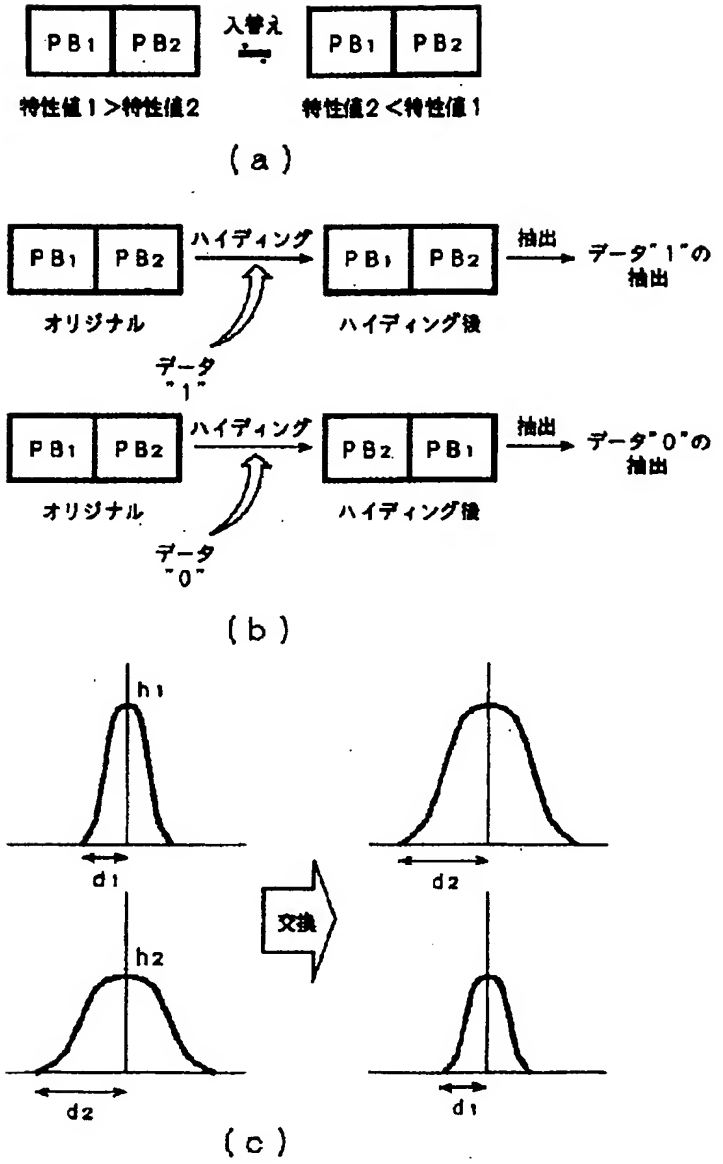
【図3】


D
(a)
分離
D1
ダイジェスト
暗号化されたダイジェスト H'
(b)
D2
(c)

【図4】


41
領域特定部
45
認証部
画像データ D'
D'
D1
42
ダイジェスト計算部
画像データ D'
OK or NG
D2
43
ダイジェスト抽出部
H'
44
復号変換部
公開鍵 PK

【図5】


PB1
PB2
入替え
特性値1>特性値2
特性値2<特性値1
(a)
ハイディング
抽出
データ"1"の抽出
オリジナル
ハイディング後
データ"1"
データ"0"の抽出
データ"0"
(b)
h1
d1
d2
交換
h2
(c)